

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re application of: David Justin Ross et al.
Serial No. 10/003,719 Examiner: Zia, Syed
Confirmation No. 2644
Filed: October 30, 2001 Group Art Unit: 2131
For: Verification Engine For User Authentication
Date: March 6, 2009

Mail Stop AF
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

PRE-APPEAL BRIEF REQUEST FOR REVIEW

Applicant requests review of the final rejection in the above-identified application. No amendments are being filed with this request.

This request is being filed with a Notice of Appeal.

This review is requested for the reason(s) stated on the attached sheet(s). Note: no more than five (5) pages may be provided.

I am the:

- ☐ applicant/inventor
☐ assignee of record of the entire interest
See 37 CFR 3.71. Statement under 37 CFR 3.73(b) is enclosed
☒ attorney or agent of record
☐ attorney or agent acting under 37 CFR 1.34

Customer No. 73552

Respectfully submitted,

STOLOWITZ FORD COWGER LLP

/MICAH D. STOLOWITZ/
Micah D. Stolowitz
Reg. No. 32,758

STOLOWITZ FORD COWGER LLP
621 SW Morrison Street, Suite 600
Portland, OR 97205
(503) 224-2170

Certificate of Mailing or Transmission

I hereby certify that this paper (along with any referred to as being attached or enclosed) is being transmitted to the USPTO via the EFS-Web electronic filing system on the date set forth below.

/ Micah D. Stolowitz /

Date: March 6, 2009

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re application of

Confirmation No. 2644

David Justin Ross

Application No. 10/003,719

Filed: October 30, 2001

For: **VERIFICATION ENGINE FOR USER
AUTHENTICATION**

Group Art Unit: 2131

Examiner: Syed Zia

Attorney Docket No. 29094/14:2

Date: March 6, 2009

ARGUMENTS TO ACCOMPANY PRE-APPEAL BRIEF REQUEST FOR REVIEW

I. Introduction

The application has pending claims 1, 3-6 and 8-21. Claims 1, 4 (systems) and claims 5, 6 (methods) are in independent form. All claims stand finally rejected as allegedly anticipated by U.S. Pat. No. 6,714,944 (“Shapiro”).¹ Applicant respectfully disagrees, and reserves its rights going forward as to all claims. However, to be brief, applicant will present arguments only with regard to claim 6 and claim 5.

II. Brief Summary of the Invention

Applicant’s invention can be used, for example, by a merchant who is providing sales “online” at an E-commerce website (15 in FIG. 2), in order to verify the identity of an online customer (1) (or “subject”) by using an intermediary “verification engine” (or *Authentex*) (10). The verification engine (10) leverages information associated with the customer which held by a

¹ See final Office action, 10/6/2008.

“Trusted Validator” (3) such as the customer’s bank or a credit bureau.² In claim 6, the Trusted Validator is referred to as a “third-party”.

The bank (3a) keeps complete control of its confidential database, but it will nonetheless respond to certain queries (6) from the Authentex (10) for the purpose of verifying that the bank’s customer is who he claims to be.³ The response does not release specific data, but rather provides an indication as to whether the subject’s response to the question(s) put to him match up with a record in the Trusted Validator’s database. (“Match Confidence” is discussed below.) The allowed queries (5) are negotiated with the bank or other third-party in advance.⁴ Please refer to **FIG. 2 Replacement Sheet**.⁵ The subject is not privy in advance to what they might be.

III. Discussion

The examiner rejected the claims as anticipated by Shapiro. “In order to demonstrate anticipation, the proponent must show “that the four corners of a single, prior art document describe every element of the claimed invention. ... But that is not the whole story ... Because the hallmark of anticipation is prior invention, the prior art reference—in order to anticipate under 35 U.S.C. § 102—must not only disclose all elements of the claim within the four corners of the document, but must also disclose those elements “arranged as in the claim.”⁶ Here, key elements are missing entirely, as explained below.

A. The Prior Art

Shapiro discloses a different system for a very different purpose. Shapiro discloses a method for a user, called a *Registrant*, to make *data that he selects* accessible to a third party, such as a potential employer, in a controlled manner. See Shapiro FIG. 2. The data may be things that would appear on a resume, for example.

According to Shapiro, data that is input by the Registrant can be vetted to the relevant party, such as a prior employer, educational institution or branch of the armed services, for

² See Specification at [0035] as amended 10/2/2007.

³ These interactions, for example between the *Authentex* and the bank (*Trusted Validator*) are electronic communications between computer servers rather than live individuals in a preferred embodiment.

⁴ A bank, for example, would want to cooperate to support its customers’ online commercial intercourse.

⁵ Filed October 2, 2007.

⁶ See *Net MoneyIn, Inc. v. Verisign, Inc.* (No. 2007-1565, decided October 20, 2008) (summary judgment of anticipation *reversed*). (Slip Op. at 15-16, footnotes and citations omitted.)

verification.⁷ Through automated queries a server system asks each of the pertinent third parties to verify that data provided by the Registrant is correct –i.e., that he really did work there, graduate from that school, serve in the Army, etc. These query results are collected and stored in a data base.⁸ The Registrant is given a confidential “identifier” or key that he can forward to an “outside user” to enable that outside user to access the Registrant’s information.

B. The Present Invention

The present invention is designed to address an entirely different problem. It is intended to enable a user such as an E-commerce website *to verify that a customer is who he purports to be* –by accessing information about the customer that is held by a trusted third-party, but *not* selected by the customer for this purpose. Rather, applicant’s method employs an intermediary (the verification engine 10 aka *Authentex*) to first query the customer for identifying information, and then use the answers from the customer to form a query to the database holder (Trusted Validator 3a) for validation of the identity of the customer.

Thus there are multiple distinctions over the prior art, including the following:

a. Data is *not* selected by the subject-customer and uploaded for storage and verification; rather, *he must respond to queries from the authentication system*.

b. Verification of the customer’s ID takes place by queries to trusted validators (third-party data base proprietors) that are pre-arranged by the validation engine and *unknown* to the subject-customer in advance.

c. Initial queries are presented *to the subject or customer*, by the Authentex verification engine. The subject’s responses are used by the validator to form an allowed query to the third-party trusted validator. That third party may respond with a “match confidence” (see claim 5 below, and claim 17) that the subject-customer, as reflected in his query responses, matches a customer record in the third-party database.

In some cases, for example for larger online transactions, the system may request “out-of-wallet” data from the subject-customer.

“Out-of-wallet data is information about you that would take you a little effort to find out, but that you probably have in your filing system or somewhere equally accessible with some effort. It includes information such as the amount of

⁷ See Shapiro at column 5, lines 1-13.

⁸ See Shapiro at column 5, lines 14-25.

the last transaction with your checkbook or credit card, the holder and amount of your mortgage, your credit rating, your bank balance, and the like.”⁹

That type of data will be available to the appropriate third-part Trusted Validator.

C. Claim 6 Limitations Compared to Shapiro

Claim 6 in part recites: “6. A method of authenticating the putative identity of a subject... comprising:

“responsive to a request from a client to authenticate the putative identity of the subject, *forming a first query to elicit from the subject at least one item of information sufficient to form one of the permitted types of queries, and sending the first query to the subject via the client;*”

Refer to applicant’s FIG. 2. See Queries 8 to the subject-customer 1. See Query Responses 9 from the subject-customer to the verification engine 10. This step is not disclosed in Shapiro. In Shapiro, a user may request verification of a subject’s information. But the system does not form a query or send a query to the subject (via the client-vendor). It does nothing of the kind. Claim 6 next recites:

“*receiving identifying information associated with the subject in response to the first query* to authenticate his identity, the received identifying information including at least one item of information sufficient to form one of the permitted types of queries;”

Shapiro does not receive identifying information “in response to the first query to authenticate his identity” because it sends NO query to the subject-customer. This step is not anticipated. Next, claim 6 recites:

“forming a permitted type of query based on the received identifying information;”

Here, one might argue that the Shapiro data validation process “forms a permitted query,” but importantly, that query is not based on information received from the subject *in response to a first query posed by the validation engine to the subject*. Therefore, this step is not anticipated.

The process described in claim 6 is illustrated in the flow diagram of FIG. 3.¹⁰

⁹ Specification at [0006].

¹⁰ FIG. 3 also includes additional steps not recited in claim 6.

D. Claim 5 and Confidence Levels

Claim 5 recites the following, again following the theme based on submitting queries first to the subject whose identity is at issue:

“5. A user authorization identity authentication method comprising the steps of:
presenting to an authentication subject one or more predefined queries, the predefined queries defined in advance by agreement with owners of each of multiple independent databases, the multiple independent databases storing identifying information about the authentication subject;
receiving from the authentication subject an answer to each of the selected at least one of the predefined queries;
presenting each answer to at least one of the multiple independent databases that has corresponding identifying information;
obtaining from the multiple independent databases an authentication confidence level for each answer; and
combining the authentication confidence level for each answer into a combined confidence level for authenticating the authentication subject.”

As explained above, there is no disclosure in Shapiro about forming and sending queries to the subject sought to be identified. In addition, Shapiro does not disclose combining the database query results into a composite confidence level for authenticating the subject. See FIG. 2: Match Confidences 7 from the Trusted Validator 3a are assembled and Authentication Confidence 14 delivered to the E-commerce (user) site 15. For at least these additional reasons, claim 5 is patentable over the reference.

For at least these reasons, the pending claims are not anticipated by Shapiro.

Respectfully submitted,

RAF Technology, Inc.

By: /MICAH D. STOLOWITZ/

Micah D. Stoloritz
Registration No. 32,758

STOLOWITZ FORD COWGER LLP
621 SW Morrison Street, Suite 600
Portland, OR 97205
(503) 224-2170